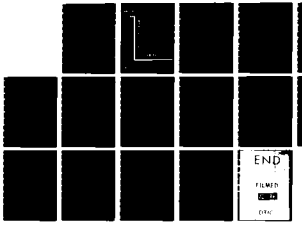
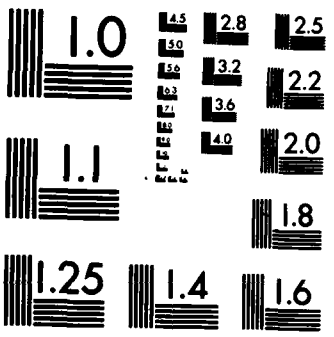
AD-A137 182 AIRCRAFT SIMULATOR: MULTIPLE-COCKPITCOMBAT MISSION TRAINER NETWORK(U) AIR FORCE HUMAN RESOURCES LAB BROOKS AFB TX J A CICERO JAN 84 AFHRL-TP-83-46 1/1

UNCLASSIFIED F/G 1/3 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AFHRL-TP-83-46

(12)

AIR FORCE HUMAN RESOURCES LABORATORY

AD A137182

AIRCRAFT SIMULATOR: MULTIPLE-COCKPIT COMBAT MISSION TRAINER NETWORK

By

John A. Cicero

OPERATIONS TRAINING DIVISION
Williams Air Force Base, Arizona 85224

January 1984
Final Technical Paper

AIR FORCE SYSTEMS COMMAND
BROOKS AIR FORCE BASE, TEXAS 78235

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely Government-related procurement, the United States Government incurs no responsibility or any obligation whatsoever. The fact that the Government may have formulated or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication, or otherwise in any manner construed, as licensing the holder, or any other person or corporation; or as conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

The Public Affairs Office has reviewed this paper, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This paper has been reviewed and is approved for publication.

MILTON E. WOOD, Technical Director
Operations Training Division

CARL D. ELIASON, Colonel, USAF
Chief, Operations Training Division

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER AFHRL-TP-83-46	2. GOVT ACCESSION NO. AD-A137182
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE *(and Subtitle)* AIRCRAFT SIMULATOR: MULTIPLE-COCKPIT COMBAT MISSION TRAINER NETWORK	5. TYPE OF REPORT & PERIOD COVERED Final
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR *(s)* John A. Cicero	8. CONTRACT OR GRANT NUMBER *(s)*
9. PERFORMING ORGANIZATION NAME AND ADDRESS Operations Training Division Air Force Human Resources Laboratory Williams Air Force Base, Arizona 85224	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 63227F 27430001
11. CONTROLLING OFFICE NAME AND ADDRESS HQ Air Force Human Resources Laboratory (AFSC) Brooks Air Force Base, Texas 78235	12. REPORT DATE January 1984
	13. NUMBER OF PAGES 32
14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*	15. SECURITY CLASS *(of this report)* Unclassified
	15.a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of this abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

cable communication
combat simulation
local area networks
tactical flight simulation
time division multiple access

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

The feasibility of a multiple-cockpit combat mission trainer (CMT) aircraft simulator is investigated. It is shown that a cable network can be used to connect many CMTs over a large geographical area. The cable channel is divided into a critical portion and noncritical portion. The critical portion uses a time division multiple access (TDMA) technique to broadcast CMT position and attitude to all other CMTs in the network. The noncritical data portion uses a random access protocol to broadcast weather, threat information, etc. An analysis technique is presented which easily evaluates the random access protocol. Suggestions for further research in this area are proposed.

DD Form 1473 EDITION OF 1 NOV 65 IS OBSOLETE
1 Jan 73

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

AFHRL Technical Paper 83-46 January 1984

AIRCRAFT SIMULATOR: MULTIPLE-COCKPIT COMBAT MISSION TRAINER NETWORK

By

John A. Cicero

OPERATIONS TRAINING DIVISION
Williams Air Force Base, Arizona 85224

Reviewed and submitted for publication by

Peter A. Cook, Lt Col, USAF
Technology Development Branch

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

PREFACE

The author would like to thank the Air Force Human Resources Laboratory (AFHRL), the Air Force Office of Scientific Research (AFOSR), and the Southeastern Center for Electrical Engineering Education for providing the opportunity to work during the summer of 1983 at Williams Air Force Base, Arizona. Also, the author would like to thank Mr. Warren Richeson and Ms. Marilyn Vickery for coordinating the appointment at Williams AFB. Lt Col Peter A. Cook and Capt Caroline Hanson provided an interesting assignment and excellent support facilities, and German exchange scientist, Mr. Uwe List, provided valuable discussions.

ABOUT THE AUTHOR

Mr. Cicero was assigned to the Air Force Human Resources Laboratory, Operations Training Division, from 1 June 1983 to 9 August 1983, under the Summer Faculty Research Program. He was selected because of his special knowledge in the field of digital communication networks gained while pursuing a doctoral degree and while teaching electrical engineering at the Illinois Institute of Technology. During the course of this study he investigated various methods for creating local area networks of flight simulators for application to the Air Force Combat Mission Trainer program.

I. INTRODUCTION

The Air Force has determined that large-scale combat simulations are necessary to maintain force readiness for future armed conflict (Cook, 1982). The increasingly complex nature of warfare demands that difficult combat missions be practiced regularly in a simulated hostile environment. It is prohibitively expensive to stage large field exercises frequently enough to provide the required experience for all personnel. Also, field exercises cannot provide actual threats such as surface-to-air missiles and antiaircraft artillery.

In 1979, a link was connected between the Advanced Simulator for Pilot Training (ASPT) at Williams AFB, Arizona, and the Simulator for Air-to-Air Combat (SAAC) at Luke AFB, Arizona. This link was limited to only two simulators and covered a maximum distance of 50 miles. The link utilized two 9600-baud telephone lines and was completely asynchronous. No security codes were included in this network, and only position and attitude data were exchanged.

A future combat mission trainer (CMT) network will link together a large number of aircraft simulators to provide the ability to practice major campaigns without loss of life or equipment and at a greatly reduced cost. The network will enable pilots to interact with all other aircraft in a strike force and to compete against enemy formations. This concept requires a network that interconnects many CMTs over a large geographical area. Individual CMT position and attitude can be transmitted to all other CMTs in the network. Also, the latest digital terrain data from the Defense Mapping Agency, threat information from various intelligence sources and satellite weather data can be transmitted across the channel.

A central computer can be incorporated in the network to provide firing status and kill/damage determination to all personnel. Also, the central computer can be used to synchronize the individual CMTs and

to determine any network faults. Once such a network is established, encrypted data transmission can be used to conduct classified combat scenarios without fear of security compromise.

II. OBJECTIVES

The main objective of this project was to investigate the feasibility of a multiple cockpit CMT network which could simulate air-to-air and air-to-surface combat scenarios. Specific objectives included (a) determining which communication channel best satisfies the CMT network concept, (b) determining the maximum separation between CMTs in a network, (c) determining how the available channel could be used most efficiently, (d) finding and evaluating a random access protocol that provides good delay/throughput characteristics for a channel with long delays, and (e) determining the effects of security on message length and channel efficiency.

III. PHYSICAL COMMUNICATION LINK AND THE CMT NETWORK

A transmission medium that provides reasonably good security, large signal-to-noise ratios, and large bandwidth must be used for the CMT network. Some possible mediums are coaxial cable, fiber optics, twisted pair, microwave, and satellite links. Twisted pair cable is susceptible to interference at high frequencies and does not provide the signal-to-noise ratios necessary for high reliability, large bandwidth communications. With microwave and satellite links, transmitted signals can easily be intercepted by an unauthorized receiver. Also, the transmission delay times for a satellite link are not acceptable in the CMT network.

Coaxial cable and fiber optics are two good mediums for the CMT network. Coaxial cable will be used as an example in this paper because it provides good bandwidth, constant received signal strength, high signal-to-noise ratio, good isolation, and reliable components and

connection techniques. Also, it is commercially installed by many Community Antenna Television (CATV) companies at competitive prices (Hopkins, 1981).

A typical CATV modem provides for point-to-point transmissions at rates of 6 Megabits per second (Mb/s) using a variety of modulation techniques. CATV supports signal-to-noise ratios of approximately 40 dB which result in uncorrected bit-error rates of better than 1 in 10^9 bits.

The CMTs can be arranged in any geographic distribution. (Figure 1 shows an example of 18 CMTs arranged in three squadrons of six, with a stand-alone central computer.) Therefore, the network will be designed such that all CMTs can communicate across a single link. This allows any possible geographic design to utilize the minimum number of links; i.e., if two squadrons are transmitting data in the same geographic

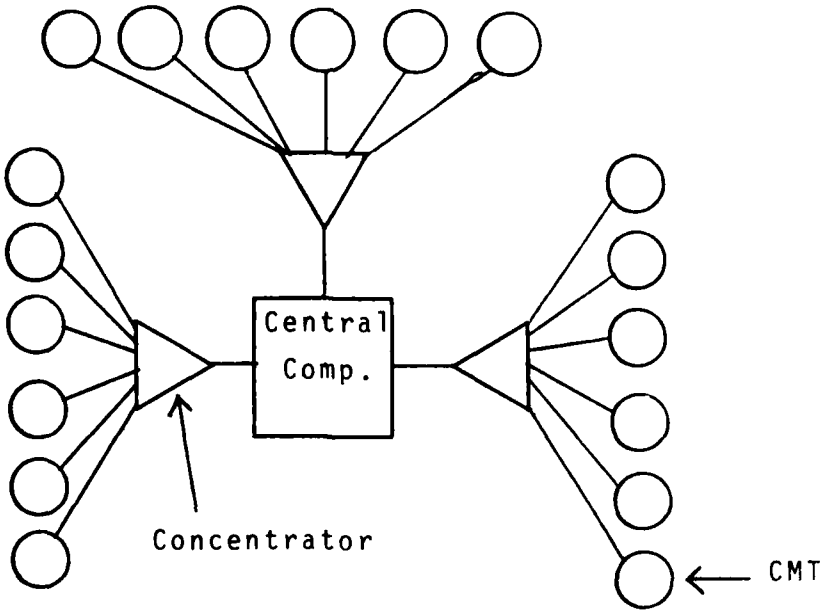


Fig. 1. An 18 CMT Network

direction, they can share a common communication link instead of requiring two separate links.

The maximum response time, T_d, from a pilot's action in one CMT to that action being displayed in another CMT must be determined by experiment. It is assumed to be 100 msec for this paper. The time required for sampling the pilot's act[illegible] T_{pa}, for processing the data at the receiving CMT, T_{rdp}, and [illegible] producing an image at each frame of the computer image generator [illegible]G), T_{c_1}, T_{c_2}, and T_{c_3} must be measured in the actual sy[illegible] Then, the maximum data transmission time from one CMT to ano[illegible], T_{dt}, can be calculated:

$$T_{dt} = T_d - T_{pa} - T_{rdp} - T_{c_1} - T_{c_2} - T_{c_3} \quad (1)$$

For example, if the following times are assumed: $T_{pa} = T_{rdp} = T_{c_1} = T_{c_2} = T_{c_3}$ = 1/60 of a second, then T_{dt} is calculated as 1/60 of a second. T_{dt} will be considered one epoch. (See Figure 2.)

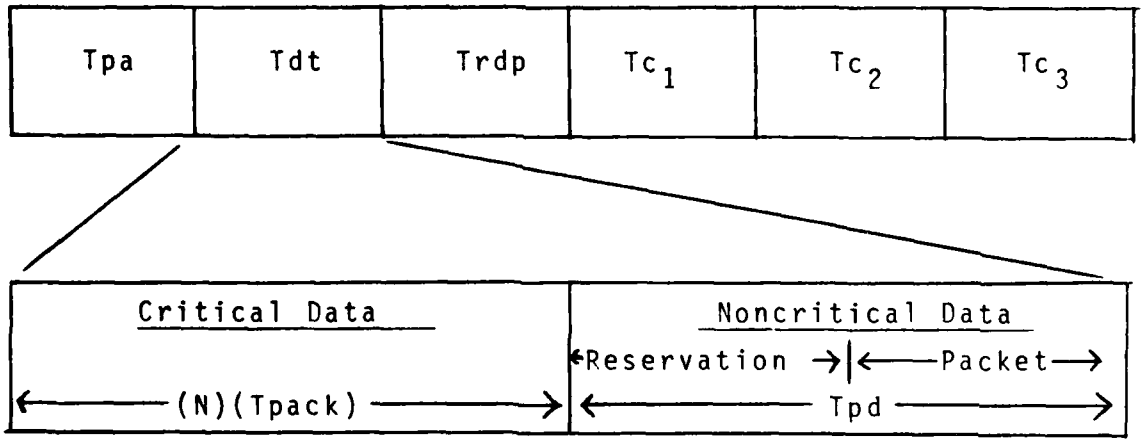


Fig. 2. System Response Times

IV. POSSIBILITY OF A SATELLITE CHANNEL

A satellite network would be desirable for long distance communications or for communications over rough terrain. The propagation delay, T_{pd}, must be calculated to see if the total transmission delay is acceptable for the CMT network.

A geosynchronous satellite must have a period equal to that of the earth's rotation, a sidereal day of 23h 56min 4.09sec (mean value). A geostationary satellite is geosynchronous with an equatorial (in the plane of the equator), near-circular, and direct (same direction of rotation as Earth) orbit. The period of an elliptical orbit is given by

$$\text{period} = 2\pi(A^3/u)^{1/2} \tag{2}$$

where A = semimajor axis of the ellipse and u = gravitational constant (Bhargara, 1981). For earth $u = 3.99 \times 10^5 km^3/S^2$. Solving for A in equation (2),

$$A = [(\text{period}/2\pi)^2 u]^{1/3} \tag{3}$$

Since the period is approximately 86,164 sec, $A = 42.2 \times 10^3$ km. Note that A (the semimajor axis of the ellipse) is the distance from the center of the earth to the satellite. Assuming that the radius of the earth, r, is approximately 6.4×10^3 km, the altitude of the satellite, h, (which is the distance between the surface of the earth and the satellite) can be computed as

$$h = A - r \tag{4}$$
$$h = 42.2 \times 10^3 \text{ km} - 6.4 \times 10^3 \text{ km} = 35{,}800 \text{ km}$$

Finally, the single-hop satellite delay (i.e., the time required to transmit a packet of information from one earth station to another via a satellite link) can be calculated as

$$T_{pd} \text{ (Single hop delay)} = 2h/c \qquad (5)$$

where c is the propagation velocity in free space (3×10^8 msec). Substituting c and h in equation (5) yields T_{pd} = 240 msec. This 240 msec propagation delay would replace the propagation delay in Figure 2 and would create a total delay, from pilot action to action displayed, of approximately 1/3 sec. A delay of this magnitude is totally unacceptable in the CMT network.

V. NEED FOR SYNCHRONIZATION

Synchronization will be extremely important for two reasons. First, the proposed communication link for this network is a single (expensive) channel. To allow many CMTs to access a single channel efficiently, the channel must be divided into different time slots. Each time slot occurs during a predetermined interval, and each CMT transmits data only during its uniquely assigned slot. This partition scheme, which is called time division multiple access (TDMA), guarantees the minimum access delay for all the CMTs in the network.

During a CMT's uniquely defined time slot, the CMT broadcasts its critical data (CMT position, attitude, etc.) to every other CMT in the network. If two or more CMTs attempt to transmit during the same time slot, a collision (mutually destructive interference) will occur, and the packets will have to be retransmitted. Collisions can be avoided if the network is well synchronized and each CMT transmits a packet only during its assigned time slot.

The second reason for synchronization is that a CIG requires one epoch to process its data, and new data cannot be processed until the current frame is completed. The processing latency can introduce an additional epoch of delay in the network response time. In a well synchronized network, data will always be presented to the CIG just

before the start of its current processing frame, thus eliminating any additional delays. Note that the pilot's stick position does not have to be sampled more often than once each T_{c_1} because the first frame of the CIG accepts new information only once each T_{c_1}.

VI. CALCULATION OF THE MAXIMUM PHYSICAL SEPARATION BETWEEN CMTs

Before the maximum physical separation between CMTs can be computed, several quantities must be determined. First a packet, length L, which is used to transmit critical data must be determined. (This packet length is independent of the packet length that will be used for noncritical data.) Next, the bit or data rate, R, must be determined. For this example, the bit rate is 6 Mb/s and the packet length is 1000 bits. Then, the time required to transmit one packet, T_{pack}, is defined as

$$T_{pack} = L/R \tag{6}$$

For this example, T_{pack} = .167 msec/packet. The time required for N CMTs to transmit one packet each is N x T_{pack} (or 3 msec for N=18).

If the total length of the data transmission slot, T_{dt}, is known, then the transmission propagation delay, T_{pd}, can be calculated. The data transmission slot is equal to the time required to transmit N packets, plus the maximum propagation delay from the transmitter to the receiver. Therefore,

$$T_{pd} = T_{dt} - N \times T_{pack} \tag{7}$$

For this example T_{pd} = 13.66 msec, and the maximum physical separation between CMTs is

$$D_{max} = (T_{pd} - D_{max}/D_{repeat} \times T_{repeat}) \times c_M \tag{8}$$

Where D_{repeat} is the average distance between repeaters;
T_{repeat} is the average propagation delay of a repeater;
c_M is the propagation velocity of the physical medium.

Solving for D_{max} in equation (8) yields

$$D_{max} = Tpd/(1/c_M + T_{repeat}/D_{repeat}) \quad (9)$$

If a repeater spacing of 1 km and an average repeater delay of 1 usec are assumed, and a propagation velocity, c_M, of 1/2 c (where c is the velocity in free space) is used, then the maximum separation between any two CMTs, D_{max} = 1781 km or 1107 miles (for the 18-CMT network). Figure 3 displays the maximum distance between CMTs versus the number of CMTs.

VII. SYNCHRONIZATION TECHNIQUES

One synchronization technique (Carter, 1980) is particularly applicable to the CMT network. Synchronization consists of a coarse and a fine search. The coarse search is applied only during the initialization of the network, whereas the fine search (or fine-tune) is continuously applied during normal data communications. (Note that during coarse search no other data communication is permitted.)

Each one of the N CMTs is assigned a unique number from 1 to N. (This same assignment is used for the unique TDMA time slots needed for the critical data communications.) The central computer generates windows during the synchronization period, where a window (or a mirror), L_w, is defined as a period of time (measured in bits) in which everything that is received by the central computer is returned to the CMTs. The length of the window is always smaller than the length of the packet (i.e., $L_w < L$). The bits at the beginning and end of the packet, L, which do not pass through the window, L_w, (and are not returned to the CMTs) are defined as gaps, L_g. The

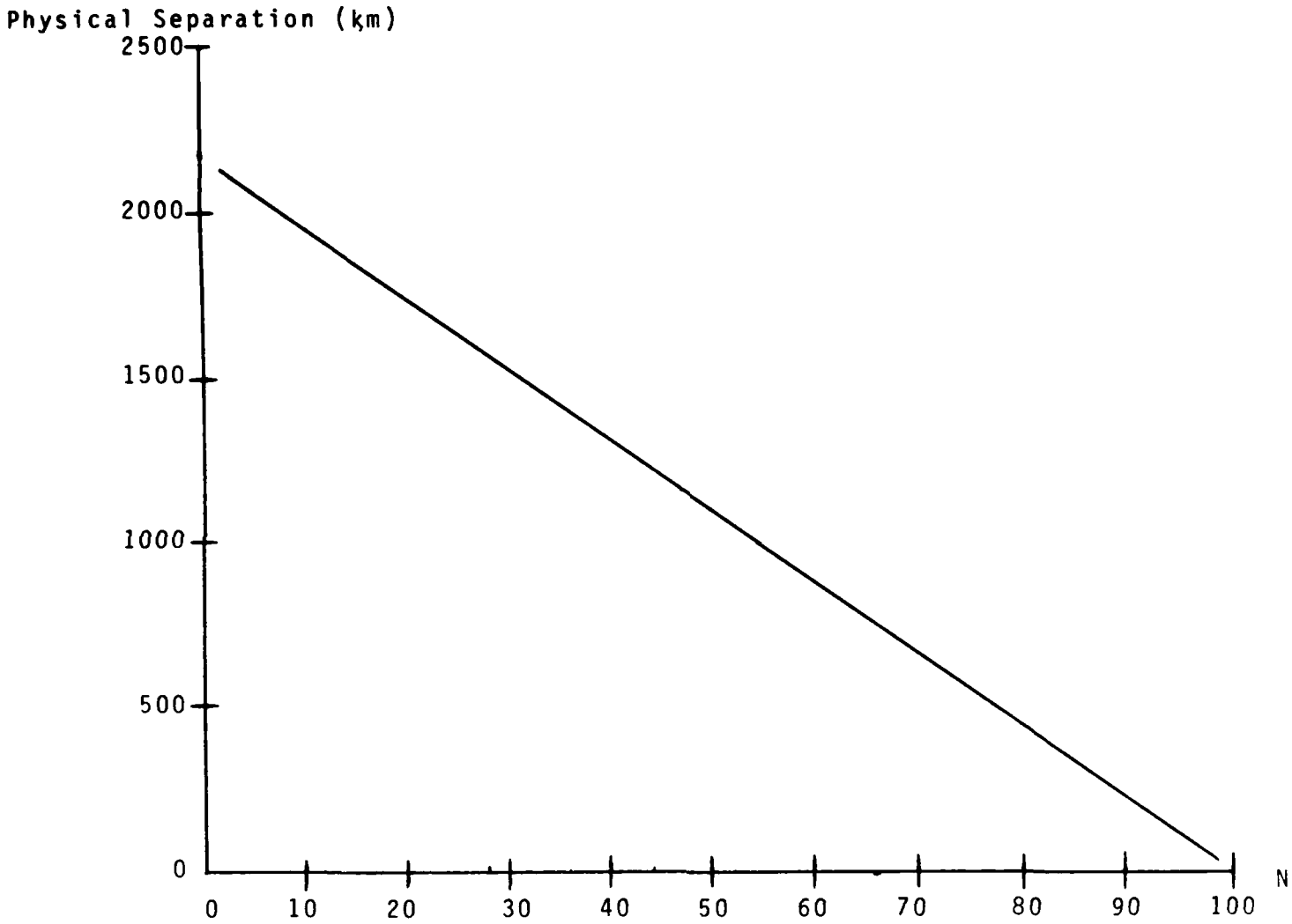


Fig. 3. Maximum Physical Separation Between CMTs versus the Number of CMTs in the Network (N) for c_M=c/2, Trepeat=1uSec, Drepeat=1km, Tdt=16.67mSec, L=1000 bits, and R=6MHz.

relationship between the window, the packet length and the gaps is defined as

$$L_w = L - 2 L_g \tag{10}$$

If the packet is defined as 1000 bits, and the window is defined as 950 bits, then two gaps (one at the beginning and one at the end of the packet) must be 25 bits each. During coarse search only one window is provided per epoch, but during normal operation, N windows are provided per epoch. The N windows provide guard bands between packets and are used for the fine search.

Coarse Synchronization begins when the central computer notifies the network that it is going to provide a window corresponding to time slot number one. During the coarse synchronization period, the central computer provides one window per epoch. This window is provided for X epochs, where X is the number of epochs needed to guarantee coarse synchronization. The first CMT will transmit a burst of L_w bits, then be idle for $2L_g$ bits. This pattern of L_w bits transmitting and $2L_g$ bits idle is repeated continuously for one epoch. Because the central computer provides only one L_w bit window per epoch, only L_w bits maximum can be returned to the transmitting CMT. Actually, when all L_w bits are returned to the transmitting CMT, the first phase of coarse synchronization for CMT number one is complete. Normally, what is returned during the first L_w bit window is a gap (of up to $2L_g$ bits maximum) somewhere in the window.

In the next few epochs, Y, the CMT must advance or retard its L_w bit bursts so that the gap is completely eliminated. At this point (which is the end of the first phase of coarse synchronization), all but one of the L_w bit bursts must be eliminated so that the unique time slot reserved by the central computer for CMT number one can be identified by CMT number one. The unwanted bursts can be eliminated by trial and error without knowing the actual distance between the CMT and

the central computer. A binary elimination scheme provides an effective elimination technique. Note that an epoch can be divided into T_{dt} x R/L L-bit slots. Therefore, the number of epochs required to eliminate the unwanted bursts, W, using binary elimination is

$$W = \log_2(T_{dt} \times R/L), \text{ and} \tag{11}$$

$$X = Y + W \tag{12}$$

In other words, a CMT should be able to locate its unique time slot coarsely in X epochs. For this example, Y is assumed to be 3 epochs, and X is calculated as 10 epochs. Simulations showed that coarse synchronization is always completed in 10 epochs or less for the network in this example.

After X epochs, the central computer must notify the second CMT to prepare for coarse synchronization, and it must move its window to the second time slot. This entire procedure is repeated for each of the N CMTs. The time required to synchronize the entire network coarsely is (N) x (X) x (T_{dt}). For this example, the network can be coarsely synchronized in 3 seconds.

Fine Synchronization begins after coarse synchronization is completed. During normal operation, the central computer provides N contiguous windows per epoch. Each window is L_w bits in length, with $2L_g$ bits between windows. Fine-tuning is performed to compensate for any drift that may occur between the clock of an individual CMT and the clock of a central computer. The fine search can be accomplished by designating the first and last L_g bits of the L_w bit packet as a pseudo noise (PN) sequence. This PN sequence will have a unique combination of 1's and 0's. When a CMT transmits a packet to the central computer, the packet is returned by the central computer to the transmitting CMT (in addition to being broadcast to all other CMTs). The transmitting CMT can compare the received PN sequence to the

transmitted PN sequence, and thus determine the accuracy of the synchronization. If the sequences are not exactly the same (due to truncation by the window), the transmitting CMT can advance or retard the start of its transmission during the next epoch to compensate for any error.

The PN sequence is used only for fine-tuning and does not contain any useful information. If some of the PN sequence does not pass through the window, the data portion of the packet will not be adversely affected. The PN sequence should be constructed such that it can easily be distinguished from the data portion of the packet. Also, it should immediately indicate the amount of correction needed to maintain synchronization. If it is assumed that a gap is interpreted as logic 0's the following PN sequence might be a useful:

GAP 1001000100001000001000000 DATA - DATA 000000100000100001000100l GAP

With this PN sequence there is a block of six logic 0's separating the data portion of the packet from the closest logic 1 in the PN sequence. This block of logic 0's is helpful in locating the start of the data portion of the packet. Also, the PN sequence gives a quick indication of the amount of information that passed through the window. For example, if 1000010 - - - is the first piece of the PN sequence that passed through the window, the receiver can immediately determine that it must retard its timing by 7 bits. Fine-tuning continuously resynchronizes the network without disrupting the critical data communications link.

VIII. NONCRITICAL DATA COMMUNICATIONS

The data communications considered in the previous sections are critical communications in the sense that every pilot's action must be displayed at every other CMT with the minimum delay. If there is

excessive delay between CMTs, the network could not be used for air-to-air or air-to-ground scenarios. However, there are other possible network communications which could tolerate some delay. For example, weather conditions could tolerate delays up to several hundred milliseconds without any noticeable degradation in network performance.

It is seen from equation (7) that there are T_{pd} seconds out of the T_{dt}-second data transmission slot in which no critical communications can be performed. During this T_{pd} second interval (which is actually the transmission delay of the critical data communications), noncritical data communications can be performed. The noncritical data are not sent to a CIG and are not affected by the CIG processing time.

Random access schemes (Tobagi, 1980) provide acceptable performance if some delays in noncritical message transmission can be tolerated. A random access or demand access protocol will be introduced which utilizes the channel efficiently for bursty (i.e., irregular) traffic in a network with large transmission delays. The noncritical data communications, together with the critical data communications, should utilize 100% of the data transmission slot in an efficient network.

This random access scheme requires a CMT to make a reservation request before it transmits its noncritical data packet. The reservation request slot, L_r, should be as small as possible to provide the most efficient noncritical communications. L_r represents the minimum number of bits necessary to discern one reservation request from another accurately. Given a physical communication link with a raw bit rate, R, a bandwidth, BW, and a carrier-to-noise ratio of C/N, L_r can be calculated according to Pritchard (1979) and Rapuano and Shimasaki (1974) as

$$L_r = (2B_r + D_c + J_1 + Q_t) \times R \qquad (13)$$

Where $B_r = 1/R$, the basic resolution or bit time of the network;

D_c is the synchronizing clock drift, approximately 6 nsec;

J_l is the logic jitter in the network, approximately 5 nsec;

$Q_t = 2/(BW \times (C/N)^{1/2})$.

For example, if R is 6 Mb/s, BW is 6 MHz, and C/N is 40 dB, then Q_t = 3.3 nsec and L_r = 2.1 bits. A reservation slot of 5 bits will be used in this example to provide an added margin of safety. Figure 2 provided an illustration of a noncritical transmission slot. The number of bits contained in this T_{pd} interval is

$$L_{pd} = T_{pd} \times R \tag{14}$$

The L_{pd} bit slot is divided into N L_r bit intervals and one L_d bit interval where

$$L_d = L_{pd} - N \times L_r \tag{15}$$

L_d is the noncritical data packet length. For this example, calculations yield L_{pd} = 82,000 bits, N x L_r = 90 bits and L_d = 81,910 bits.

In this random access scheme N CMTs compete for a single L_d bit slot every epoch. Since each CMT will not have noncritical data to transmit every epoch, this random access scheme is employed. The TDMA scheme, used for critical data, results in excessive average delays when the input traffic to the network is bursty.

Each CMT is initially assigned a number from 1 to N. During the first epoch, any CMT that has information to transmit makes a reservation request during its assigned reservation time slot. For example, if CMTs five and seven have information to transmit during the first epoch, they will each transmit an L_r bit reservation request during the fifth and seventh reservation time slots, respectively. Note that the reservation requests consist only of an L_r bit carrier burst (i.e., no modulated information is sent during the reservation slot). At the beginning of the second epoch, all CMTs examine the requests made during the first epoch. The reservation request closest to slot one wins the right to transmit its data packet during the second epoch. All the losers from the first reservation epoch, together with all the new messages generated during the first epoch, make new reservation requests during the second epoch's reservation slot.

In a priority reservation scheme, the reservation requests in subsequent epochs follow the same priority assignments as in the first epoch. The CMT with the lowest fixed assignment will always win the right to transmit its data first.

In a random reservation scheme, the priority of every CMT in the second epoch will vary from the priority in the first epoch according to the following algorithm: new assignment = $(\text{old assignment})_{\text{MOD N}} + 1$. Similarly, the priority assignment of subsequent epochs is modified according to this alogrithm. It should be noted that if a packet collision is detected (possibly due to an error in synchronization), the CMTs will revert to their original assignments of a number from 1 to N.

With either scheme, the reservation process continues in every epoch. Requests are always made in the previous epochs for the right to transmit data during the present epochs. CMTs continuously make reservation requests until they win the right to transmit their packets.

Assume that every CMT has packet generations that follow a Bernoulli distribution and that packets cannot be generated by a busy CMT (i.e., CMTs contain a single packet buffer). A CMT generates a new packet with probability, p, and remains idle with probability, 1 - p. Also, assume that a packet can be generated by the CMT only if the CMT's packet buffer is empty at the beginning of the epoch. This transmission scheme can be modeled as a Markov process. Figure 4 shows an example of the possible states in which a four-CMT network can be found during one embedded Markovian interval. The designation u_i indicates that there are i CMTs at the beginning of an embedded Markovian interval waiting to transmit a packet to the network during the interval. Since time is slotted (i.e., the network is synchronized), the system can be described by the following Markov chain:

$$u(t + 1) = A\, u(t) \tag{16}$$

where t represents discrete time, $u(t) = [u_0(t), u_1(t), \ldots, u_N(t)]^T$ is the state probability vector, the sum of all u_i states equals 1, and A is the state transition matrix.

The structure of Figure 4 shows that u_i cannot be decreased by more than one packet per epoch (since there is a maximum of one packet transmission per epoch) and that the network cannot move from state u_i to state u_4 $(i > 0)$ because busy CMTs cannot generate new packets. Noting that transmissions and arrivals are a function of the state of the network at the beginning of the embedded Markovian interval, a general state transition matrix, A, is obtained as

$$A^T = [a_{ij}] \tag{17}$$

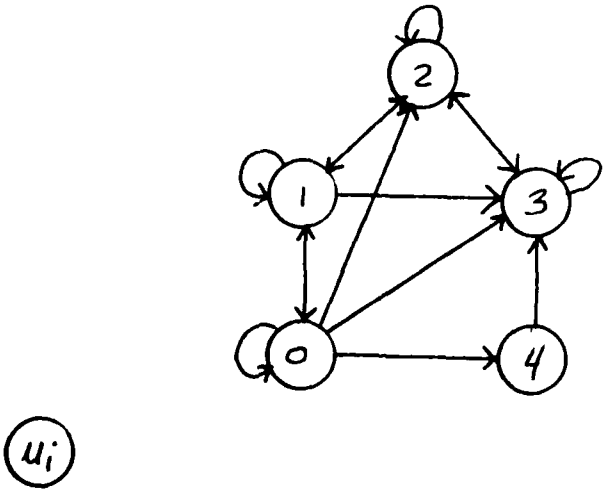


Fig. 4. Possible States of a Four CMT Network

where a_{ij} represents the probability of moving from state i to state j during one embedded Markovian interval. A general formula for a_{ij} for a network of N CMTs is

$$a_{ij} = 0, \text{ for } k > N - i \text{ or } i > j + 1, \text{ and}$$

$$a_{ij} = \binom{n - i}{k} p^k (1 - p)^{N - i - k}, \tag{18}$$

Where $k = j$ for $i \leq 1$, and $k = j - i + 1$ for $i > 1$.

The steady state solution of equation (16), denoted as u^*, can be obtained by substituting (18) into (17) and (17) into (16), then solving (16) iteratively until $u(t + 1) = u(t)$. The average steady state throughput, S, is defined as the average number of packets transmitted during one Markovian interval. S is computed as

$$S = \sum_{i=1}^{N} u_i^* \tag{19}$$

The average number of busy CMTs in the network, G, is

$$G = \sum_{i=1}^{N} i\, u_i^* \tag{20}$$

The average delay time for packets to reach their destination is

$$\text{Delay} = (G/S + 1)T_{dt} \text{ sec} \tag{21}$$

Solving equation (16) becomes increasingly difficult for large CMT networks. For a 100-CMT network, a 100 by 100 array is required. To eliminate this problem, an averaging technique was investigated. Meerkov (1980) showed that a stochastic system can be represented by a deterministic averaged equation such as

$$y(t+1) = y(t) + (P_{arr}(t) - P_{tr}(t))/N \tag{22}$$

where (N)(y(t)) represents the average number of busy CMTs in the network at time t, N is the total number of CMTs in the network, $P_{arr}(t)$ is the average number of new packets generated during one epoch, and $P_{tr}(t)$ is the average steady state throughput. It can be shown mathematically that $P_{arr}(t)$ is equal to (1 - y(t))(N)(p), where p is the Bernoulli probability of arrival used in (18). It was determined experimentally that $P_{tr}(t)$ is equal to (1 - exp[-y(t)]). Then equation (22) can be rewritten as

$$y(t+1) = y(t) + ((1 - y(t))(N)(p) - (1 - \exp[-y(t)]))/N \tag{23}$$

From the definition of G and S it can be seen that G = (N)(y) and S = P_{tr}. Simulations were run to verify the predicted results, and average errors of less than 4% were obtained.

IX. DATA SECURITY IN THE CMT NETWORK

The effect of a security code (Davis, 1981) on packet length and transmission delay will be presented. A data encryption algorithm can utilize pseudo-random number generators, which generate uniformly distributed random numbers over a period of time that is considerably shorter than the period of the random number generator. The random number generator is called "pseudo-random" because the next random number is generated by applying an algorithm to the present random number. In other words, the sequence of numbers generated by the pseudo-random number generator is not really random; it just appears random over a period of time that is shorter than the period of the generator. When the transmitting CMT and the receiving CMT use the same algorithm in their pseudo-random generators, the encrypted message can easily be decoded. (The encrypted message generated by the transmitting CMT, does not appear to be random at the receiving CMT since both CMTs follow the same deterministic algorithm.) However, if an unauthorized receiver does not know the encryption algorithm, the received information will appear to be random.

A pseudo-random number generator requires an initial "seed" (or number) from which it can generate a random sequence of numbers. The transmitting CMT and receiving CMT must use the same initial seed (and the same algorithm) to exchange information properly. A problem with this scheme is that the seed (or key) must be secretly transmitted to all CMTs in the network before communication can begin. The advantage of this scheme is that with sophisticated encryption algorithms an unauthorized receiver could know the algorithm but still not be able to decode the received sequence because the seed is not known.

This random number is added (modulo two) to the original data at the transmitting CMT and subtracted (modulo two) from the received message at the receiving CMT. This encryption scheme does not increase

the length of the original data (see Figure 5) and the amount of delay added to the network is negligible.

The feasibility of a multiple-CMT network over a large geographical area hinges on the question: "How secure is a secure network?" Certainly the sophisticated encryption codes available today could not be decoded in real time without the aforeknowledge of the encryption algorithm and the initial seed. However, given enough time (i.e., possibly days, weeks, months, etc.), most (if not all) encryption schemes could be cracked. This means that the data transmitted during CMT combat scenarios could be received and saved by the enemy and eventually decoded (at which time the entire scenario could be reenacted).

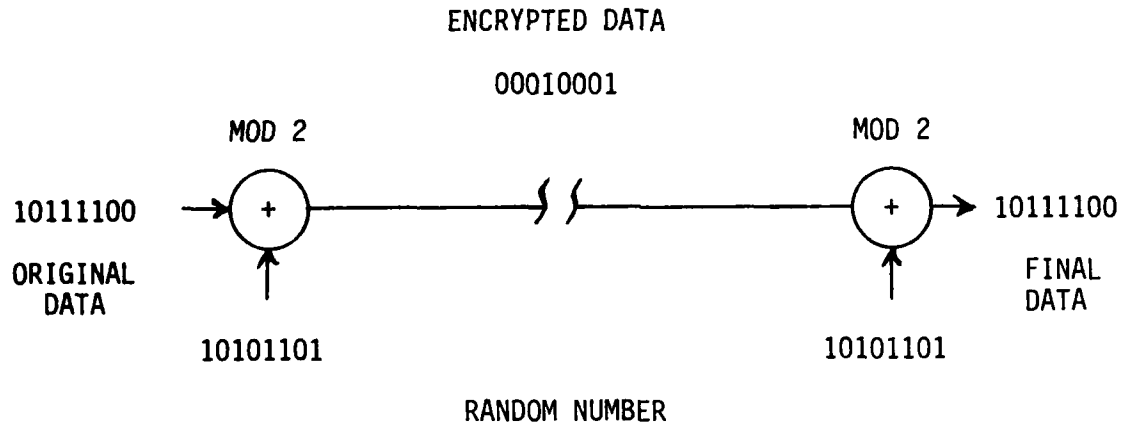


Fig. 5. A Data Encryption Scheme

This problem of unauthorized receivers essentially eliminates microwave, satellite, and telephone links because there is easy access to these channels. The cable network could be secured by enclosing it in some type of protected conduit which must be capable of detecting a break in the line.

X. NETWORK COST

The approximate network cost can be computed for a cable network (excluding CMTs and computers). Assume that the network has a single link connecting two nodes (each node may contain several CMTs). If a maximum distance of 1100 miles (calculated earlier) is used and connection costs of $200 per repeater and $5 per foot of installed unsecured cable are assumed, then the cost of the network is 1100 repeaters (approximately one per mile) @ $200 each, plus 1100 miles of cable @ $5 per foot, yielding a total cost of $29,260,000.

Certainly, existing networks could be used for a fraction of the cost, but it would be difficult to guarantee secure communications. It should be noted that a cable of this type typically has 300MHz of usable bandwidth. The 6-MHz bandwidth used by the CMT network occupies only 1/50 of the total available bandwidth. Therefore, many channels of audio and video could be added to this cable to make it more cost effective. For example, the images seen by all the pilots could be sent to a central location to be evaluated by the instructors.

XI. RECOMMENDATIONS

This paper presents two results. First, the feasibility of a CMT network is described. Second, a random access protocol for large delay networks is presented and evaluated. The protocol was evaluated using a traditional Markov chain and a simple approximation technique.

Future work could include the actual implementation of this network. Several CMTs could be connected at a single site with delays introduced to emulate an actual network. Response times could be measured and the random access protocols could be tested.

From a theoretical point of view, the evaluation technique presented in this paper should be extended to a CMT network with multiple packet buffers. The approximation technique would produce M equations instead of one equation, where M is the number of packets per CMT. Stability, delay, and throughput could then be evaluated for any possible CMT network with any size packet buffers.

REFERENCES

Bhargava, V. K., (1981). Digital Communications by Satellite. New York: Wiley and Sons, Inc.

Carter, C. (1980). Survey of synchronization techniques for a TDMA satellite-switched system. IEEE TRANS. COMM., 8 (vol. COM-28), 1291-1301.

Cook, P. A. (1982). Aerial combat simulation in the U.S. Air Force. Astronautics and Aeronautics, 9, 60-65.

Davis, D. W. (1981). Data security in computer networks. In S. Ramami (Ed.), Data communications and computer networks (pp. 45-56). New York: North-Holland Publishing Co.

Hopkins, G. T. (1981). Local computer networking on CATV coaxial cable. In S. Ramami (Ed.), Data communications and computer networks (pp. 275-279). New York: North-Holland Publishing Co.

Meerkov, S. M. (1980, December). Decentralized control by rational controllers. Journal of Optimization Theory and Applications, 32, 499-520.

Pritchard, W. L. (1979). Satellite communications -- An overview of the problems and programs. In H. L. Van Trees (Ed.), Satellite communications (pp. 2-15). New York: IEEE Press.

Rapuano, R. A., & Shimasaki, N. (1974). Synchronization of earth stations to satellite-switched sequences. Communications Satellite Technology, 33 (Progress in Astronautics and Aeronautics), 411-429.

Tobagi, F. A. (1980). Multiaccess protocols in packet communication systems. IEEE TRANS. COMM., 4 (vol. COM-28), 468-488.